Bank of Ghana's Experience in Implementing Cybersecurity Policy Frameworks & the Coordination Models Adopted to Build a Robust Ecosystem

Alliance for Financial Inclusion High-Level Joint Learning Programme on Inclusive FinTech Ecosystems and Cybersecurity (Virtual)

7th October 2020

Remarks by Mrs. Elsie Addo Awadzi, 2nd Deputy Governor, Bank of Ghana

1. Technology has become the biggest driver of change in the financial services sector. With significant investments in technology, financial services providers are providing convenience and efficiency for customers and helping to expand access to finance for underserved and unserved segments of society.

2. Technology is also making financial services even riskier, as a result of fraud and other risks that could affect operations, financial soundness and stability, and confidence in the financial system.

3. Risks to financial inclusion are also pronounced. Digital financial services (DFS) have become a key catalyst to increased financial inclusion especially for the informal sector, women, youth and other typically underserved groups. However, increased cyber risks could also lead to service delivery disruptions, operational losses and reputational damage for service providers, while leading to losses for users of these services and a loss of confidence in the financial system. These could erode gains made in financial inclusion in the developing world.

4. In the midst of the pandemic, there has been an increase in the use of DFS. The incidence of fraud and attempted fraud has also increased in particular in the mobile money space but also in ATM and other payments-related fraud.

5. Key issues to be addressed from a regulatory perspective to help anticipate, identify, and mitigate cyber risks on a continued basis include:

    a. Improvements in the security systems and infrastructure of national switches, banks and other financial services providers, electronic money issuers, telcos, fintechs including 3rd party aggregators and technology service providers;
    b. Deploying staff and other insiders in fraud prevention and mitigation;
    c. Enhancing capacity to understand, identify and mitigate cyber risks on the part of operators, regulators, security agencies, and the entire national eco-system
    d. Enhancing cross-border regulatory cooperation (regional and global) in respect of financial institutions, telcos, fintechs operating in multiple jurisdictions.

6. The Bank of Ghana's approach to addressing cyber risks in the banking and payments ecosystem is designed to safeguard operational resilience, safety, soundness, and integrity of the entire system while promoting confidence in the use of financial services (including DFS) and financial inclusion. To this end, the Bank of Ghana has taken the following measures:

    (i) Issued the Cyber and Information Security Directive (CISD) in 2018 which provides for:

    - Governance requirements for financial services providers to institute key risk mitigation pillars – including a Board Committee on information security matters, senior management roles including Internal Audit and Chief Information Security Compliance Officer (CISO), among others;
    - Technical requirements to augment security including ISO27001 certification and adoption of ISO27032, PSI-DSS compliance for

institutions that handle, process, store, or transmit debt card, credit card, prepaid card, e-purse, ATM Cards etc.

- Reporting by regulated entities on a periodic basis and as and when incidents occur.

(ii) Our regulatory approach enables payment service providers (e.g. electronic money issuers, fintechs, and others) to participate in the payments and DFS ecosystem to help generate innovate products and services, but in a manner that ensures that regulatory requirements are proportional to the risks that are likely to be introduced into the system. For very small financial service providers and fintech, the burden of regulatory requirement is relatively low, but to avoid regulatory arbitrage, their access to payments infrastructure is through bigger and more established service providers.

(iii) BoG's comprehensive Risk-Based Supervisory Framework ensures that cyber security issues are embedded in the supervisory cycle for licensed financial services providers as part of operational risks assessments and overall safety and soundness assessments. Cooperation among all of BoG's supervisory Departments overseeing banks, specialized deposit-taking institutions (e.g. savings and loans companies, microfinance companies, and others), and payment systems infrastructure and service providers. A coordinated approach is in place to ensure that risks that cut across are identified and mitigated in a comprehensive manner.

(iv) BoG stresses continued vigilance for all service providers and operators in the ecosystem, as well as continually educates consumers to help empower them to take steps to protect their financial transactions especially those that are digital.

(v) BoG also stresses the need for enhanced due diligence in recruitment and outsourcing by financial institutions and payments systems operators and service providers, to mitigate insider fraud.

(vi) BoG has strong cooperation arrangements with key domestic stakeholders. Cyber security is a key national priority, and governance structures and strategies are in place with leadership at very high levels of Government. Sectoral cyber security policies and strategies exist. Within the financial sector, BoG implements policies, strategies, and regulation for the banking and other deposit-taking institutions and payments system infrastructure and service providers. Information is shared between BoG and the national authorities frequently. BoG engages with other financial sector regulators bilaterally and at the level of the Financial Stability Council whose mandate is to promote regulatory cooperation, financial system-wide risk mitigation, and crisis preparedness.

7. Going forward, cross-border cooperation remains an issue to explore to promote information sharing and harmonized approaches to regulating cross-border service providers. Also, continuous capacity building in the industry and for our supervisory teams will be key, while enhanced consumer education will help to empower consumers to make choices that protect their financial assets and livelihoods.